United Nations S/2015/376

Security Council

Distr.: General
28 May 2015

Original: English

Letter dated 26 May 2015 from the Chargé d'affaires a.i. of the Permanent Mission of Burundi to the United Nations addressed to the President of the Security Council

I have the honour to submit to you a press release by the Government of the Republic of Burundi concerning its position on the crisis currently faced by the country (see annex).

I kindly request that the present letter and its annex be circulated as a document of the Security Council.

(*Signed*) Anésie **Ndayishimiye**
Chargé d'affaires a.i.

15-08422 (E) 040615

Please recycle

Annex to the letter dated 26 May 2015 from the Chargé d'affaires a.i. of the Permanent Mission of Burundi to the United Nations addressed to the President of the Security Council

Position of the Government of Burundi on the crisis currently faced by the country

The Government of Burundi appreciates the concerns of the international community and the region about the crisis in the country. The Government of Burundi notes that, even before the current crisis, Burundi had been over the past year a subject of discussion by the Security Council more often than other countries facing conflicts and humanitarian crises. The reports designed to paint the Government in a bad light have now evolved with the international media and foreign agents engineering and fanning demonstrations as well as an exodus of refugees from border areas.

The recent attempted coup played into that plot and was intended to ensure the establishment of a transitional Government in Burundi. Despite those attempts, which only history will judge, Burundi, as a responsible member of the international community, has opened its doors to all those who may honestly wish to find the truth. The Government believes that the facts on the ground would negate the reports circulated in the international media and which regrettably shape international and regional opinion.

The Government of Burundi is, however, deeply concerned about the ongoing diplomatic activity that tends to undermine and, to a large extent, disrespect the constitutional institutions of Burundi. While the Government welcomes delegations of special envoys and committees of eminent personalities to assist in finding solutions to the current crisis, it regrets that these delegations come with preconceived ideas and recommendations that are not informed by the facts on the ground. In that regard, the Government of Burundi wishes to outline its position on various aspects of the crisis that should serve as a guide and an advisory to all delegations that seek to engage on those matters.

The Government wishes to emphasize that, while it appreciates the advice of all those concerned, some matters that touch on sovereignty, constitutionality and the rule of law that governs the Republic of Burundi may not be subject to discussion. The following position should therefore serve as a guide.

Candidacy of President Nkurunziza

The Government of Burundi wishes to emphasize that there is a need to respect the constitutional institutions of Burundi. In that regard, the Government of Burundi will not negotiate or discuss matters that tend to undermine those institutions. This is the red line that must guide those seeking to engage in discussions with the Government. President Nkurunziza has reiterated that, if elected, this will be his last term, as established in the Constitution.

Demonstrations

The truth must be told. Those demonstrations which the Government believes to be sponsored are small in number and limited to four suburbs of Bujumbura. The

demonstrators are under instructions to create violence to elicit a violent reaction from the Government. The Government is aware of this and has exercised restraint, despite the deaths of police and military officers and injuries to many others.

Media

Burundi has had the most open and free media in the region, with Burundians freely airing their views on the many private radio stations. Nevertheless, with the current crisis, that freedom has been abused as the radio stations have become agents of those wishing to start an insurrection in the country. The Government is, however, working with all stakeholders to create a code of conduct to be adhered to by the media and journalists, particularly during the electoral process and in this time of crisis.

Electoral process

The Government of Burundi believes that it is only through the democratic process of holding elections every five years that the people of Burundi can freely choose their leaders. The voice of the silent majority not demonstrating in the streets should be heard through the ballot box.

The Government appreciates the decision of the Electoral Commission to postpone the local and legislative elections, as was requested by various stakeholders, such as political parties, independent candidates, religious confessions, the region and the international community.

Support to the electoral process

The Government of Burundi appreciates the support received to date from friendly Governments and international organizations for holding the elections. Nevertheless, it has a responsibility to ensure that the democratic culture of holding periodic elections in Burundi takes root and, while requesting additional support, will conduct the elections with the limited resources at its disposal.

Refugees

The refugees who are crossing over to neighbouring countries are Burundians. The Government of Burundi is more concerned about their welfare than anybody else. The genesis of that crisis stems from the fearful memory of what happened to them in 1993 more than from any actual violence happening now. The refugees going to Tanzania were victims of atrocities at the hands of the then Burundian army. The perpetrators of that massacre are well known. The fears and scars have not healed. The refugees going to the Democratic Republic of the Congo are recent returnees who are fearful of being targeted as being members of the Interahamwe or the Forces démocratiques de libération du Rwanda. The recent attack on an innocent man suspected by demonstrators of belonging to the Interahamwe has led to that fear.

The refugees going to Rwanda are made to believe that the crisis in Burundi will lead to a tribal conflict and that the Interahamwe will target them. The rumours that trigger those fears are no doubt the work of foreign agents, the opposition and those from civil society that wish to create such a scenario.

Dialogue

The Government of Burundi is open to dialogue with Burundians, especially, as usual, within the forum of political parties, the international community and countries in the region, on the way forward to address the current crisis. Such dialogue should be held with the Government's position in mind. Already, under the auspices of the Special Envoy of the Secretary-General of the United Nations and the African Union, such dialogue is ongoing. The Government, however, advises that the voice of the majority of the Burundians, who reside in rural areas, must be taken into account.

The United Nations, the East African Community, the International Conference on the Great Lakes Region and the African Union must send fact-finding missions to the rural areas of Burundi, where the majority of Burundians live, and not base their opinion on the few demonstrators, biased members of civil society and the opposition parties whose leaders stay mainly in Bujumbura.

Coup attempt

The Government regrets that the coup attempt took place, leading to the deaths of some Burundians. The Government appreciates the support of the international community and the regional organizations that promptly condemned the attempted coup and called for the respect of constitutionality. The Government is committed to ensuring that the arrested coup-plotters face a fair judicial process. The Government further calls upon those on the run to surrender, as they will be treated fairly by the justice system in Burundi.

Role of the international community and the region

The Government requests the international community and the region to play the following role in order to address the crisis:

(a) To support an all-inclusive electoral process and urge the parties that have submitted candidates to fully participate in the elections. The Government commits itself to providing a level playing field and security to all candidates;

(b) To send fact-finding missions to the border areas from which the refugees originate to determine the actual cause of the exodus;

(c) To urge neighbouring countries to contribute positively to peace and stability in Burundi and to facilitate the return of refugees, so that they may enjoy their civil right to vote. More than 99 per cent of the territory of Burundi is indeed peaceful;

(d) To respect the constitutional institutions of Burundi and the constitutional timelines as regards the electoral process. Indeed, with regard to the presidential election calendar, the Government informs the people and the international community that the date remains unchanged. As a matter of fact, the Constitution and the Electoral Code provide that the election of the President of the Republic takes place at least one month and two months at most before the expiration of the term of the President of the Republic (art. 103 of the Constitution). It should be recalled that the swearing-in of the President of the Republic may not take place beyond 26 August 2015;

(e) To send observer missions to assess the climate and the conduct of the elections;

(f) To prevail upon those sponsoring and encouraging the demonstrations to call them off, so that the elections may take place in the four areas of Bujumbura.

Done at Bujumbura, on 22 May 2015

Office of the Spokesperson and the Secretary-General
of the Government

United Nations S/2015/377

Security Council

Distr.: General
26 May 2015

Original: English

Letter dated 26 May 2015 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism addressed to the President of the Security Council

On behalf of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism, I have the honour to submit to the Security Council a report entitled "Gaps in the use of advance passenger information and recommendations for expanding its use to stem the flow of foreign terrorist fighters", which was prepared pursuant to the request made in the statement of the President of the Security Council of 19 November 2014 (S/PRST/2014/23).

The Committee would appreciate if the present letter and the report were brought to the attention of the members of the Security Council and issued as a document of the Council.

(*Signed*) Raimonda **Murmokaitė**
Chair
Security Council Committee established pursuant to
resolution 1373 (2001) concerning counter-terrorism

15-08234 (E) 050615

Please recycle

Gaps in the use of advance passenger information and recommendations for expanding its use to stem the flow of foreign terrorist fighters

I. Summary and introduction

1. The present report provides an examination of the use of advance passenger information (API) systems by Member States, with a view to identifying gaps and capacity-building needs. In response to the threat posed by foreign terrorist fighters to international peace and security, the Security Council adopted resolution 2178 (2014) on 24 September 2014. In the resolution, among other things, the Council requires Member States to prevent individuals believed to be foreign terrorist fighters from entering or transiting through their territories (para. 8).[1] In paragraph 9, the Council calls upon Member States to require that airlines operating in their territories provide API to the appropriate national authorities in order to detect the departure from, or attempted entry into or transit through, their territories, by means of civil aircraft, of individuals designated by the Security Council Committee pursuant to resolutions 1267 (1999) and 1989 (2011) concerning Al-Qaida and associated individuals and entities.

2. Elaborating on the obligations set forth in the resolution, the Security Council issued a presidential statement on 19 November 2014 in which it, among other things, requested the Counter-Terrorism Committee Executive Directorate to prepare an analysis of the gaps in the use of API by Member States and to make recommendations to expand its use (S/PRST/2014/23). The present report is submitted in accordance with that request.

3. In its simplest form, an API system is an electronic communications system that collects a passenger's biographical data and basic flight details provided by an airline operator. The data are generally collected from the passenger's passport or other government-issued travel document. Typically, the data are transmitted to border control authorities for various checks before the arrival of a flight.

4. API is similar to, but distinct from, passenger name record systems, which the Security Council encouraged Member States to use. Passenger name record systems consist of information, such as ticketing details and itineraries, collected from passengers by travel management systems when flights are booked. The data are thus not based on a government-issued travel document and may not contain important identifying information such as date of birth or gender.

5. Currently, only 51 Member States (or slightly more than a quarter of the membership of the United Nations) use API systems, which can be an effective tool in interdicting the travel of foreign terrorist fighters, other terrorists and individuals engaged in transnational organized crime, especially when used in conjunction with databases of the International Criminal Police Organization (INTERPOL).

---

[1] Foreign terrorist fighters are defined in the preamble of the resolution as individuals who travel to a State other than their State of residence or nationality for the purpose of the perpetration, planning or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training, including in connection with armed conflict. It should be noted that the resolution was adopted pursuant to Chapter VII of the Charter of the United Nations and is therefore binding on all Member States.

6. To illustrate the potential benefits of API in interdicting foreign terrorist fighters and other individuals engaged in criminal activity, we may take the simple example of an individual travelling by air through a transit country to participate as a foreign terrorist fighter in a conflict such as that in the Syrian Arab Republic. Where API is in use, data can be collected from that individual's passport at the point of departure, at the check-in stage. The information will be checked by border control agencies and then transmitted to the authorities in the country of destination. If the check reveals that the traveller's name appears on any INTERPOL watch list, the authorities in the arrival or transit country will have the information necessary to determine an appropriate course of action, i.e., to intercept and question the individual or detain him or her for further questioning, depending on the circumstances. Without the use of API, the disruption of the individual's travel by air would be unlikely and he or she would be able simply to proceed unimpeded to join the conflict in the Syrian Arab Republic.

7. There are numerous reasons for the low incidence of API use. First, the systems are complex and therefore require a high degree of technical capacity and skill. A further technical complication is that there are multiple types of API systems. Airlines must therefore put in place various systems and protocols in order to communicate in all API formats. In addition, the systems are expensive to purchase, maintain and operate. Furthermore, the collection and use of passenger information may raise concerns relating to individual privacy rights and may require suitable oversight and regulation by States.

8. The present report provides a description of the methodology of the Counter-Terrorism Committee Executive Directorate in collecting information on the use of API, an overview of API systems and the various types of systems currently in use and a discussion of the use of passenger name record systems, which are similar to, but distinct from, API systems and could supplement API for better risk analysis and determining the appropriate course of action. An analysis of the gaps in the use of API by Member States follows. It is noted that only 51 States currently use API, notwithstanding its potential to interdict foreign terrorist fighters and to enhance border and aviation security generally. Lastly, and based on the gap analysis, the Executive Directorate makes recommendations aimed at expanding the use of API and enhancing its effectiveness for those Member States that already use it.

9. The Counter-Terrorism Committee Executive Directorate makes 12 recommendations in response to the challenges and gaps that it has identified in connection with expanding the use by Member States of API. They are intended to increase the overall number of States using API, as required by the Security Council in its resolution 2178 (2014), and to maximize the value of API from a security perspective for those States that currently use it.

10. Generally, the 12 recommendations are designed:

(a) To raise awareness among Member States of the Security Council's call to implement API systems and the potential benefits of API systems;

(b) To enhance the collection of information concerning the use of API by Member States;

(c) To strengthen the use of API as a tool to stem the flow of foreign terrorist fighters;

(d) To compile good practices in the use of API;

(e) To request the Counter-Terrorism Committee Executive Directorate to facilitate the development of plans and projects aimed at implementing API systems;

(f) To encourage donor support for the implementation and operation of API systems by Member States.

11. Following the Committee's adoption of the recommendations, the Counter-Terrorism Committee Executive Directorate will undertake to work in close cooperation with other international organizations such as the International Air Transport Association (IATA), the International Civil Aviation Organization (ICAO), the International Organization for Migration (IOM) and the World Customs Organization (WCO). The Executive Directorate will also undertake to keep the Committee updated on the status of API system implementation by Member States.

12. It should be noted that API alone cannot prevent the travel of foreign terrorist fighters. It is one tool that can be used to make it more difficult for fighters to travel freely. A comprehensive border management strategy aimed at stemming the inter-State travel of fighters should include other elements, such as an integrated approach to border management; effective control of porous borders; measures to tackle the use of evasive travel patterns (or "broken travel" — the deliberate use of techniques to break long-distance travel into multiple segments so that it becomes difficult to ascertain travel history and travel origin); improved and consistent use of the INTERPOL I-24/7 global police communications system and stolen and lost travel documents database; possible screening of transit passengers by immigration control; and providing front-line officers tasked with regulating the movement of persons across borders with updated information and tools to conduct effective evidence-based travel risk assessments and screenings to help to identify foreign terrorist fighters.

II. Context and methodology

13. To obtain information for the present report, the Counter-Terrorism Committee Executive Directorate distributed, on 6 February 2015, a questionnaire to all 47 Member States known to be using API in accordance with the IATA database at the time of distribution. The main purpose of the questionnaire was to generate a coherent picture of how API systems are currently used internationally and to determine where gaps in use currently exist. Member States were asked seven general questions concerning the sanctions lists and watch lists against which they match API, when the matching occurs and how the matching is conducted (see annex II). Owing to the self-reporting nature of the IATA database, it was difficult to track the exact number of Member States that had implemented API systems. Since the distribution of the questionnaire, IATA has informed the Executive Directorate that four more Member States have reported using API, bringing the total number to 51.

14. Of the 47 Member States surveyed, the following 23 responded to the questionnaire: Antigua and Barbuda, Australia, Barbados, Canada, China, Dominica, Grenada, Guyana, Jamaica, Japan, Myanmar, New Zealand, Panama, Romania, Russian Federation, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Switzerland, Trinidad and Tobago, United Kingdom of Great Britain and Northern Ireland, Ukraine and United States of America. Their responses have been incorporated into the present report. In view of the increase in terrorist-related activities worldwide (including by foreign terrorist fighters who, according to some

estimates, number between 15,000 and 20,000, and possibly as many as 30,000)[2] and the adoption of Security Council resolution 2178 (2014), there is much room for improvement in the provision of information on this topic by Member States.

15. In preparing the present report, the Counter-Terrorism Committee Executive Directorate consulted the Analytical Support and Sanctions Monitoring Team established pursuant to resolution 1526 (2004), IATA, ICAO and the Stimson Center (a think tank with expertise in API-related matters).

III. Advance passenger information: a significant border control tool

16. The concept of API was developed in 1993 by IATA and WCO to address the dramatic growth in airline passenger transport. API was intended to increase border control, arrival and, where applicable, departure processing efficiency, while also reducing the workload of the law enforcement officials protecting ports of entry and exit.[3] In the light of the growing threat posed by terrorism, a driving force behind the expansion of API has been the enhancement of border security through the provision of advance warning of persons of interest travelling to a country. In the absence of API, not only is a Government's border security compromised, but also its border control strategy is largely reactive because its ability to manage risk, gather and analyse intelligence, monitor trends and share passenger information with other countries is significantly diminished.

17. An API system is an electronic communications system that collects passenger biographical data and basic flight details provided by the airline operator. The data are generally collected from the passenger's passport or other government-issued travel document. Airline communication networks then transmit the data to border control agencies in the destination country or country of origin, where outbound API recording is mandated either before the flight's departure or its arrival at the airport of destination. Once transmitted, the data are then, in practice, checked by the relevant border control agencies against various sanctions lists and watch lists used for immigration, customs and security purposes. If the data are received before the flight's departure, border control agencies can also use API as a decision-making tool to assist Member States in determining whether a passenger should be permitted to board an aircraft.[4]

18. Before the adoption of resolution 2178 (2014), the Security Council had not called upon Member States to require airlines operating in their territories to provide API. Annex 9 to the Convention on International Civil Aviation requires any Contracting State introducing a requirement for API systems in its national legislation to adhere to internationally recognized standards for the transmission of API. Annex 9 also states that, when specifying the identifying passenger information to be transmitted, Contracting States are limited to requesting only data that are available in machine-readable form, in travel documents conforming to the applicable specifications. Furthermore, all information required must conform to specifications.

---

[2] S/2014/815, paras. 14 and 88.

[3] IATA, ICAO and WCO, "Guidelines on advance passenger information (API)", 2013, paras. 1.2 and 1.3. Available from www.icao.int/Security/FAL/Documents/1.API%20Guidelines%202013%20Main_%20Text_E.pdf.

[4] Ibid., para. 3.8.

19. In 2013, IATA, ICAO and WCO jointly published[5] updated guidelines on API with the goal of establishing best practices for Member States and aircraft operators seeking to implement API systems.[6] The guidelines outline the maximum set of API data that should be included in the message for transmission to border control agencies in the destination or departure country (para. 1.6) and recommend that, in requesting passenger data, Member States limit their requirements to the minimum necessary according to national legislation (para. 8.1.2).

IV. Non-interactive batch-style systems versus interactive systems

20. API systems vary significantly in complexity, depending on costs, technical specifications and level of security. In this regard, they may be divided into two distinct categories: non-interactive batch-style API systems and interactive API systems. Each has its own unique operation and application. At the simplest level, API may involve an airline operator providing the border control agencies of the destination country with passenger manifests for the purpose of conducting checks on passengers before their arrival. At a more complex level, interactive API may be used. This allows passenger data to be exchanged between the computer system of an airline operator and those of the border control agencies of the destination country using real-time communication, thereby enabling the identification of high-risk passengers before they board a flight.

A. Non-interactive batch-style systems

21. Non-interactive batch-style API systems collect all passenger and crew data during the check-in process and transmit it as a single message at the moment of departure or just thereafter.[7] Some States, however, mandate that API data for flight crew be extracted, formatted and transmitted as an entirely separate message. The requesting Government generally receives API well in advance of the flight's arrival, giving it ample time to perform sufficient checks of all inbound passengers against relevant sanctions lists and watch lists before landing.[7] Having ample time available to perform checks enables border control officers to scrutinize close name matches in order to maximize accuracy in identifying passengers of interest and also allows for further checks on particular passengers to be performed when necessary. This reduces instances of incorrect detention or questioning of arriving passengers. Upon arrival, border control officers are able to identify passengers of interest for further questioning or deny them entry into the country, as appropriate. This also allows passengers to be efficiently processed through immigration without unnecessary delays.

---

[5] The WCO mandate for API standardization stems from Annex J1 to the revised Kyoto Convention on the Simplification and Harmonization of Customs Procedures, which seeks internationally standardized API. The ICAO mandate regarding the introduction and implementation of API systems comes from articles 22 and 23, in particular, and articles 13 and 37, generally, of the Convention on International Civil Aviation. The interest of IATA in API lies essentially in enhancing and streamlining the border-control process applied by government agencies in respect of arriving or departing passengers and crew.

[6] IATA, ICAO and WCO, "Guidelines on advance passenger information (API)", para. 1.7.

[7] Ibid., para. 5.2.

22. While passengers clearly reap the benefits of non-interactive batch-style API systems upon arrival in their countries of destination, one shortcoming of those systems is that they are less effective in enhancing aviation security because of their limited ability to identify and interdict high-risk passengers before a flight's departure.

B. Interactive systems

23. As an alternative to the non-interactive batch-style API system, Member States can elect to adopt an interactive API system, which captures passenger data during the check-in process and allows the data to be simultaneously transmitted to the relevant border control agencies in the destination country. After the data have been received by the border control agencies, a risk assessment is conducted in near real-time, indicating whether the passenger is authorized to board or whether further checks must be conducted.[8] Interactive API can be used to stem the movement of foreign terrorist fighters across borders and prevent fighters and high-risk passengers from boarding an aircraft. It thus functions as both a border security tool for the destination country and an aviation security tool.

24. Interactive API systems are much more complex than non-interactive batch-style API systems and therefore require more comprehensive network protocols.[9] The costs and technical complexity involved in establishing and implementing an interactive API system mean that very few countries have chosen to adopt the more technologically complex interactive approach. Currently, only 12 of the 51 Member States that have implemented an API reporting requirement effectively operate interactive API systems.

25. Given that interactive API systems require the destination country to approve passengers before they board a flight, it is important that airline check-in processes not be negatively affected. Border control agencies must therefore conduct passenger checks in a timely manner and provide responses promptly. Current users of interactive API aim to complete submission, evaluation and response within four seconds per transaction.[10]

C. Passenger name record: an additional tool to support the use of advance passenger information

26. In addition to emphasizing the importance of API, the Security Council encouraged the use of passenger name record systems (see S/PRST/2014/23, para. 16). "Passenger name record" is the generic name given to a record generated by airline operators or their authorized agents for each flight booked by, or on behalf of, a passenger.[11] A passenger name record is created from data supplied by the passenger concerning all segments of a journey. The data are usually supplied weeks before the scheduled journey and include a passenger's full travel itinerary and information such as seating requests, meal preferences, health issues and

[8] Ibid., para. 5.5.

[9] Ibid., para. 5.7.

[10] Ibid., para. 5.6.

[11] ICAO, *Guidelines on Passenger Name Record (PNR) Data* (2010), para. 2.1.1. Available from https://www.iata.org/iata/passenger-data-toolkit/assets/doc_library/04-pnr/New%20Doc%209944%201st%20Edition%20PNR.pdf.

additional services requested. It should be noted, however, that a passenger name record does not necessarily include a passenger's date of birth or gender. At least one of those details is needed, in addition to the passenger's name, to be able to conduct matching with watch lists to a reasonably accurate degree. Furthermore, unlike API (which is based on government-issued identity documents) the passenger name record is not verified, because it is supplied by the traveller.

27. Although passenger name records were initially used as a commercial airline management tool to assist airlines in providing passenger services, they are also used by border control agencies for counter-terrorism and transnational crime prevention and interdiction purposes. When used effectively, passenger name record data can supplement API, allowing for better analysis by authorities of the risk that certain passengers represent, as well as in improving the understanding of travel patterns and trends, such as the use of broken travel by foreign terrorist fighters. Industry standards governing passenger name records are detailed in the IATA *Passenger Services Conference Resolutions Manual* and in the Airlines for America/IATA *Reservations Interline Message Procedures — Passenger*.[12]

28. The table shows the similarities and differences between API and passenger name records.

Similarities	*Differences*
• Both are in the form of electronic data, shared through secure communications.	• API is generated during check-in or at flight closure.
• Both contain data pertaining to the passenger and to the flight on which he or she will arrive or depart.	• API derives information from government-issued documents, whereas information fed into passenger name records is unverified by the authorities.
• Both contain data viewed as useful for intelligence-driven border control and law enforcement.	• A passenger name record is generated at booking and at other specified intervals before scheduled departure and then at departure.
• Both are usually carried out on the basis of a bilateral agreement that addresses privacy and/or international human rights safeguards.	• A passenger name record includes much more data (may include some or all API data elements), but does not necessarily include date of birth or gender, whereas API does.
	• While passengers are required to provide all elements of API, they are not required to provide all passenger name record elements, such as meal preferences and health issues.
	• Passenger name records raise more privacy or international human rights law issues because, unlike API, the data collected would not necessarily otherwise be presented upon arrival.

[12] Available from www.iata.org/publications/Pages/pscrm.aspx and www.iata.org/publications/Pages/AIRIMP.aspx, respectively.

V. Gaps in use by Member States

29. On the basis of research conducted for the purposes of the present report, the Counter-Terrorism Committee Executive Directorate has identified key challenges that need to be overcome in order to address gaps in the use of API by Member States effectively. They are:

(a) Ensuring timely and accurate data transmission between the airline operator and the requesting Member State;

(b) Interoperability of the transmitted data with the inter-agency database or databases of the destination country;

(c) Accurate matching of passenger data with relevant watch lists;

(d) Use of API for risk and trend analysis;

(e) Costs involved in developing and maintaining a functioning API system;

(f) Legal and regulatory challenges concerning passenger privacy and data protection.

A. Technical challenges faced by Member States

30. API is technically complex and its use requires a high level of expertise. Challenges encountered in the process of matching passenger data against watch lists and the transmission of data to their intended recipient are major barriers to the adoption by Member States of API and its effective use as a tool to prevent the movement of foreign terrorist fighters.

Transmission of data

31. Although airline operators and border control agencies must connect their networks so that passenger data can be transmitted and received electronically, many face challenges in implementing such technology owing to its complexity and its high cost.

32. Because of the lack of uniformity across passenger data systems and message formats, Governments must use information technology systems that have the capability to send and receive all the required message formats. Developing a system that complies with such highly technical and varied requirements places a huge burden on airline operators and Governments, both financially and technologically, and is a challenge that many Member States are currently unable to meet.

33. In receiving API, the destination country must designate a first point of collection to which airline operators can transmit the data (i.e., a single window). Member States have experienced difficulties in doing so, and this, in turn, can undermine the forwarding of data to relevant border control agencies, such as immigration and customs, in the destination country. Furthermore, where border control agencies in the receiving country use independent operating systems, API may need to be converted into a format that is compatible with the system of the receiving agency before it can be screened against the relevant sanctions lists and

watch lists or processed by authorities for risk assessment purposes.[13] Otherwise, the same data must be sent multiple times to each agency in the same or differing formats. This requires additional resources, increases the time needed for processing and increases the costs incurred by Governments and airline operators.

34. To achieve the full benefits of API, airline operators and Governments must adopt and implement best practices to ensure that accurate data for each passenger on a covered flight are collected, verified and transmitted to the destination country. Such practices include ensuring that airline operators verify the identities of passengers against current travel documents before boarding and confirming that data in the travel document of an individual passenger match the data collected electronically.[14]

Matching passenger data against watch lists

35. Regardless of whether batch or interactive API is in use, API systems must be able to interact with the national border security systems of the implementing country, including intelligence and risk analysis systems, border management information systems and immigration or visa information systems. When screened against the information contained in those systems as part of an analysis of risk potential, API can be used to inform border control agencies whether a particular passenger should be prohibited from boarding a flight or intercepted upon arrival in the destination country.

36. For the screening to be thorough and efficient, the name matching software, which is used to match passenger names against watch lists (including national and regional watch lists and those maintained by INTERPOL), must be adequate. All Member States surveyed by the Counter-Terrorism Committee Executive Directorate indicated that they had infrastructure and software capabilities enabling them to automatically match watch lists against API. Eight Member States have opted to independently design and build their own API matching systems. Other Member States, such as the countries of the Caribbean Community (CARICOM), use commercial API systems that have been tailored to their specific national requirements.

37. API is matched against various lists maintained by border control agencies after passengers have already boarded their flight and are en route to their destination country. This post-departure/pre-arrival system of API matching is used in every Member State that responded to the questionnaire, with the exception of Australia, the United Kingdom and the United States, which have the ability to conduct matching before departure, owing to their implementation of interactive API systems.

38. Pre-departure matching of passenger data at airports may add time to the check-in process. However, changing risk factors, such as the increased threat of terrorism, may make such operations necessary because they can enable border control agencies to prevent high-risk passengers from boarding flights at all.[15] Results from the questionnaire indicate that the lack of pre-departure matching is a major gap in the use of API.

39. The questionnaire also reveals the need for strengthened cooperation among Member States when matching API against various lists. The data collected from the questionnaire show that, once passenger data are captured and transmitted to border

[13] WCO, IATA, ICAO, "Guidelines on advance passenger information (API)", para. 6.4.3.
[14] Ibid., para. 5.10.
[15] Ibid., para. 5.8.1.

control agencies in the destination country, they are almost always matched only against the destination country and INTERPOL watch lists, even though countries have access to other sanctions lists and watch lists, such as United Nations lists, regional and multinational lists, lists provided by partner Governments and lists developed by Member States themselves.

40. According to the questionnaire data, all but two Member States surveyed routinely match all passenger data against the INTERPOL watch lists. Only New Zealand, Switzerland, Ukraine, the United Kingdom and the CARICOM countries indicated making use of regional lists, however. Canada uses a watch list provided in conjunction with a partner Government (known as "Tipoff U.S.-Canada" or "TUSCAN"), but this practice has not been adopted by other Member States surveyed. These examples of inter-agency cooperation demonstrate that a higher level of international cooperation is achievable. This can assist in eliminating unnecessary processing duplication while ensuring the best use of existing information.

B. Financial costs and resource commitments

41. Developing, implementing and maintaining an API system inevitably involves significant financial costs and commitment of resources for both Governments and airline operators. The upfront costs are largely associated with system development and integration, as well as the purchase and installation of infrastructure, but continuing costs also stem from the capture and transmission of passenger data, upgrades to the system (to ensure that watch lists are current), general maintenance, ongoing operation and the need for sufficient supporting resources.[16] In addition, the international community must ensure that IATA is adequately supported from both a financial and a resource perspective so that it can support Member States requiring additional assistance in developing API systems.

42. Implementing interactive API systems presents a considerably greater degree of complexity than non-interactive batch-style API systems. The associated costs are therefore much higher and the time needed to fully implement functioning interactive API systems is significantly longer.[17] Even though most international airline operators already have functioning interactive API capability, Member States lag behind. Only 12 currently have interactive API capability. As more Member States implement API systems, it is anticipated that the costs will fall, thereby making such systems gradually more affordable and thus more widely accessible.

43. There are measures that can be used to reduce costs in implementing API systems, including the possibility of airline operators capturing passenger data at the time of booking, the use of machine-readable passports[18] and the signing of agreements that encourage Governments and airline operators to work together in implementing an API system (as is the case in Australia).[19]

---

[16] Ibid., para. 6.4.6.

[17] Ibid., para. 5.9.

[18] According to the Standards and Recommended Practices on Facilitation of ICAO (annex 9 to the Convention on International Civil Aviation), standard 3.10.1, "for passports issued after 24 November 2005 and which are not machine readable, Contracting States shall ensure the expiration date falls before 24 November 2015".

[19] WCO, IATA, ICAO, "Guidelines on advance passenger information (API)", para. 6.5.1.

C. Legal and regulatory challenges faced by Member States

44. Member States that begin to implement API systems in furtherance of resolution 2178 (2014) must consider how to ensure compliance by airlines with the requirement to use API. Methods to ensure compliance will inevitably vary depending upon national conditions and considerations. The use of API could be mandated by national law (whether through legislative acts or through regulations, depending on the constitutional structure of the Member State) and compliance could be coerced through various measures, including through fines imposed on airline operators.[20]

45. Resolution 2178 (2014) includes a requirement that any measures taken by Member States to counter terrorism comply with all their obligations under international law, in particular international human rights law. One legal challenge faced by Member States in the effective implementation and use of API concerns the right to be protected by law against unlawful or arbitrary interference with privacy in the context of passenger data collected, retained, transmitted and used (art. 17 of the International Covenant on Civil and Political Rights and art. 12 of the Universal Declaration of Human Rights).

46. According to the United Nations High Commissioner for Human Rights, the implementation of API systems raises important considerations regarding the right of individuals to be protected by law against unlawful or arbitrary interference in their privacy, as well as against discrimination. Member States must therefore ensure that any measure that interferes with privacy comports with their international obligations and commitments; that procedural safeguards and effective, independent oversight are in place to guard against discriminatory measures and/or the abusive use of personal data; and that there are avenues for redress available in the event of abuse (see A/HRC/28/28, para. 53).

47. Although the laws of Member States inevitably vary, they generally include provisions regarding the rights of individuals in relation to their personal data.[21] Common challenges in this regard include references to the disclosure of personal data to third parties and provisions concerning the transmission of personal data across national borders and beyond the jurisdiction of the country in which the data were collected.[22] National laws should and do address the potential conflict between API obligations, on the one hand, and privacy and data protection laws, on the other. There have been instances in which the lack of international consistency in passenger data protection has resulted in significant problems for airlines operating flights internationally. For example, international airline operators may be faced with the choice between refusing to transmit passenger data, in violation of the requirements of API laws of the departure or destination country, or providing the

[20] Recommendation (f) addresses this aspect of the legal challenges.

[21] Where such legislation incorporates obligations concerning personal data undergoing automated (computer) processing, it frequently requires that personal data should be obtained and processed fairly and lawfully; be stored for legitimate purposes and not used in any way incompatible with those purposes; be adequate, relevant and not excessive in relation to the purposes for which they are stored; be accurate and, where necessary, kept up to date; and be preserved in a form that permits identification of the data subjects for no longer than is required for the purposes for which that data is stored. See WCO, IATA, ICAO, "Guidelines on advance passenger information (API)", para. 9.4.

[22] Ibid., para. 9.5.

data, in breach of the data protection requirements of the departure or destination country. In addition, passengers may be concerned about the manner in which their personal information will be handled.

48. However, given that API systems give border control agencies the ability to gain access to passenger data that would otherwise be presented by the passenger to immigration authorities for inspection at the time of passenger arrival (essentially the data contained in the machine-readable zone of a passenger's passport) the transfer of API to third parties is perhaps not the main legal concern in implementing API systems internationally. Expanded access to passenger data gives border control agencies more time to perform relevant checks and determine whether passengers should be interdicted.[23] Issues relating to privacy and data protection potentially raise greater concerns regarding retention of passenger data and the use of such information for purposes other than national security or passenger clearance.[24]

49. With regard to the use of passenger data after its collection by border control agencies, there are concerns about passengers who have been incorrectly matched against watch lists or flagged as high-risk individuals. Where there are no guidelines stating how long this information may be held by border control agencies and for which other purposes it may be used, there are potentially long-term consequences for passengers.

50. The Counter-Terrorism Committee Executive Directorate is aware that Member States have demonstrated that implementing effective API systems that overcome many of the aforementioned challenges is an achievable goal.

VI. Recommendations

51. On the basis of the above analysis, and in the light of the requirements of resolution 2178 (2014) and the presidential statement of 19 November 2014, the Counter-Terrorism Committee Executive Directorate recommends the following:

(a) **The Committee should conduct a high-level briefing for all Member States, in conjunction with senior officials of IATA, ICAO and WCO, to facilitate awareness-raising among Member States of the need to implement API systems and to draw attention to the relevant internationally agreed standards and best practices;**

(b) **The Chair of the Committee should participate in the next IATA annual general meeting to highlight the important role played by the airline industry in ensuring the implementation of API systems, in partnership with Member States, and to highlight areas of cooperation with the Committee;**

(c) **The Committee should request the Counter-Terrorism Committee Executive Directorate to engage in IATA and ICAO awareness-raising and joint-messaging efforts concerning the benefits of API systems for evidence-based traveller risk assessment and screening procedures, including at regional events;**

[23] Ibid., para. 9.1.

[24] Ibid., para. 9.6.

(d) Noting the challenges faced by IATA in its collection of information on the status of API system implementation by its members through a voluntary reporting system, the Security Council should request the Counter-Terrorism Committee Executive Directorate, in collaboration with IATA, to serve as the global focal point for collecting information on the status of API system implementation by Member States;

(e) Noting the significant costs to and technological constraints on each Member State in developing and implementing customized API systems, the Security Council should request that IATA, ICAO and WCO:

(i) Actively encourage Member States seeking to implement an API programme to comply with existing agreed standards and best practices;

(ii) Develop a plan to review and modernize existing standards and processes that will enhance API programme efficiency and effectiveness;

(f) The Committee should encourage Member States to introduce legal mechanisms, including measures to promote compliance by airline operators, into national legislation to promote compliance with international standards for API transmission;

(g) The Committee should encourage Member States currently using API systems to consider implementing pre-departure matching of passenger data at airports for the purpose of identifying individuals, before their departure, who may be travelling abroad as foreign terrorist fighters;

(h) The Committee should request IATA to compile a guide on best practices and lessons learned from the experiences of Member States that have already implemented API systems;

(i) The Committee should encourage the Counter-Terrorism Committee Executive Directorate to continue to fulfil its role to facilitate, through its dialogue with and visits to States, the delivery of technical assistance aimed at strengthening capacity in this area;

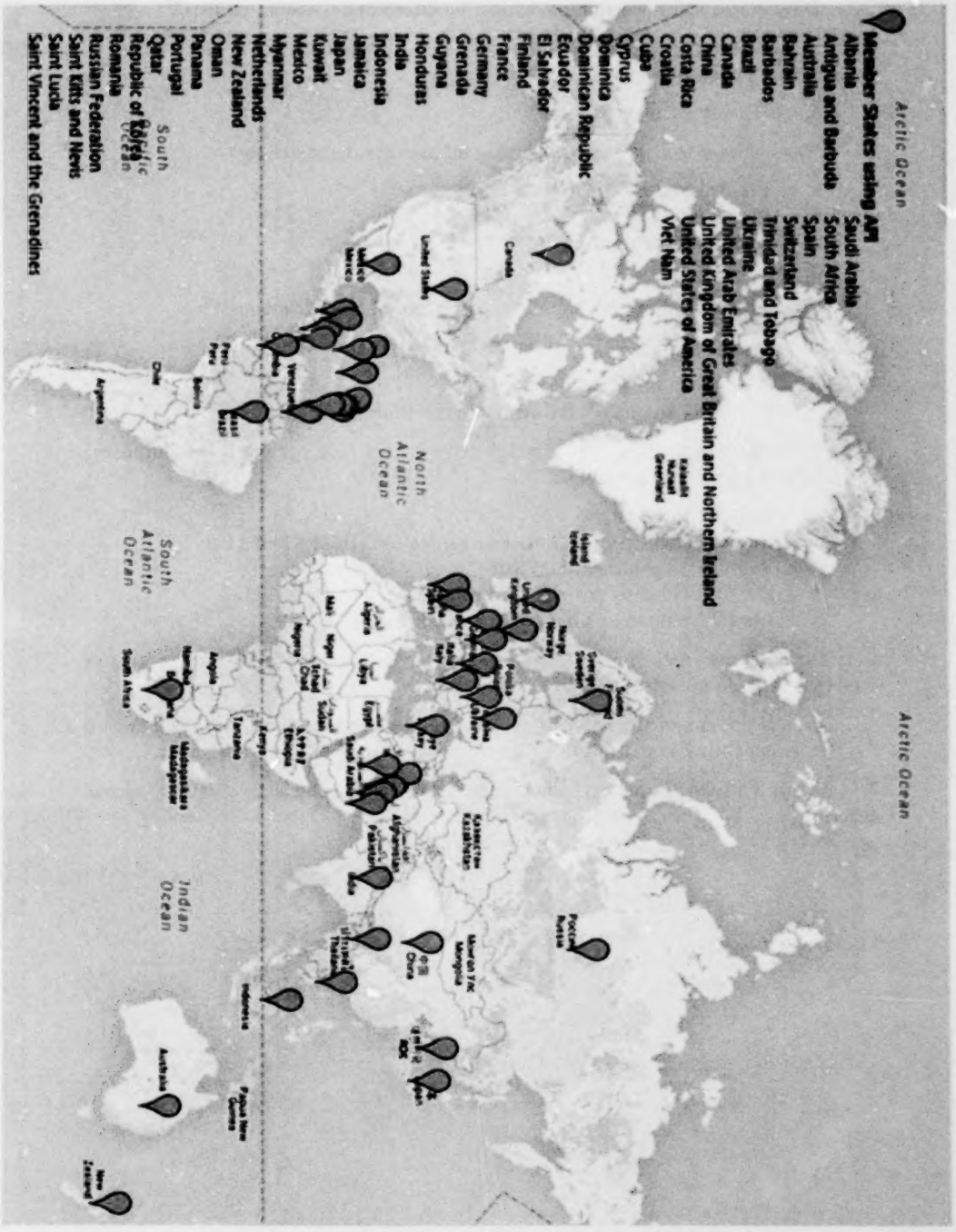
(j) The Committee should request the Counter-Terrorism Committee Executive Directorate to facilitate, in consultation with the Counter-Terrorism Implementation Task Force, the development of plans and projects with IATA, ICAO, IOM and WCO aimed at assisting with the implementation of API systems, with a particular focus on States affected by the foreign terrorist fighter phenomenon;

(k) The Committee should encourage donor entities and assistance providers, including the Counter-Terrorism Implementation Task Force, to support the above-mentioned initiatives and other activities to be undertaken by IATA, ICAO, IOM and WCO in support of the implementation by Member States of API systems in line with the requirements of Security Council resolution 2178 (2014);

(l) The Security Council should request the Counter-Terrorism Committee Executive Directorate to continue monitoring trends in the implementation by Member States of API systems and to report, within 365 days, to the Committee on the status of API implementation.

Annex I

Map of Member States using API



Annex II

Questionnaire

1. Do you use API for matching against sanctions and other watch lists?

2. If the answer to 1 is "yes", do you do this for all travellers or for a subset of the traveller population?

    a. If a subset, please specify.

3. If the answer to 1 is "yes", when do you perform the matching?

    a. Pre-departure
    b. Pre-arrival
    c. At primary processing
    d. Other

4. If the answer to 1 is "yes", is the matching automated or manual?

    a. If the answer to 4 is "automated", did you:

        i. Build the matching system?
        ii. Buy commercially available matching software?

5. If the answer to 1 is "yes", which lists do you use for matching purposes? (please be as specific as possible):

    a. United Nations lists
    b. International Criminal Police Organization (INTERPOL) lists
    c. Regional or multinational lists
    d. Lists provided by partner Governments
    e. Lists developed by your own Government

6. Do you use API for risk assessment — to identify potentially high-risk travellers who do not appear on any sanctions or watch list?

    a. If the answer to 6 is "no", would you be interested in developing such a capability in the future?

7. Do you use API for any other purpose not identified above? If so, please describe.